SEVENTH FRAMEWORK PROGRAMME
Theme SEC-2011.2.5-1 (Cyber attacks against critical infrastructures)

D3.3 Legal and Architectural Feedback

Contract No. FP7-SEC-285477-CRISALIS

Workpackage	WP 3 - Validation Support
Editor	J.-U. Bußer
Version	1.0
Date of delivery	M24
Actual Date of Delivery	M24
Dissemination level	Public
Responsible	SIE
Data included from	Davide Balzarotti (IEU), Irina Besekow (SIE), Damiano Bolzoni (UT), Jens-Uwe Bußer (SIE), Marco Caselli (UT), Jacob Fritz (SYM), Erwin Kooi (ALL), Michael Munzert (SIE), Heiko Patzlaff (SIE), Daniela Pestonesi (ENEL), Fabienne Waidelich (SIE), Ricarda Weber (SIE), Emmanuele Zambon (SM)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n°285477.

SEVENTH FRAMEWORK PROGRAMME

Theme SEC-2011.2.5-1 (Cyber attacks against critical infrastructures)

The CRISALIS Consortium consists of:

Symantec Ltd.	Project coordinator	Ireland
Alliander		Netherlands
Chalmers University		Sweden
ENEL Ingegneria e Innovazione		Italy
EURECOM		France
Security Matters BV		Netherlands
Siemens AG		Germany
Universiteit Twente		Netherlands

Contact information:
Matthew Elder
Symantec Limited
Ballycoolin Busines Park (GA 11-35)
Blanchardstown
Dublin 15
Ireland

e-mail: matthew_elder@symantec.com

Contents

1 Motivation and Scope **8**

2 Properties of Developed Crisalis Tools **9**
2.1 Tool Avatar 9
2.2 Tool Access Miner 11
2.3 Toolset Smart Fuzzers 13
2.4 Tool FCScan 13
2.5 Tool Flow Fingerprinter 15
2.6 Tool Distributed Network Monitoring 17
2.7 Tool FERRET 18

3 Use Cases and Requirements **21**
3.1 Use Cases 21
3.2 Requirements 22
3.2.1 Ethical and Legal Requirements 22
3.2.2 Technical Requirements 28
3.2.3 Usability Requirements 29

4 Applicability Analysis **30**
4.1 Tool Avatar 30
4.1.1 Ethical and Legal Aspects 30
4.1.2 Technical Aspects 33
4.1.3 Recommendation Summary 34
4.2 Tool Access Miner 35
4.2.1 Ethical and Legal Aspects 35
4.2.2 Technical Aspects 36
4.2.3 Recommendation Summary 36
4.3 Toolset Smart Fuzzers 37
4.3.1 Ethical and Legal Aspects 37
4.3.2 Technical Aspects 39
4.3.3 Recommendation Summary 40

4.4 Tool FCScan . . . 40
4.4.1 Ethical and Legal Aspects . . . 40
4.4.2 Technical Aspects . . . 42
4.4.3 Recommendation Summary . . . 42
4.5 Tool Flow Fingerprinter . . . 42
4.5.1 Ethical and Legal Aspects . . . 42
4.5.2 Technical Aspects . . . 45
4.5.3 Recommendation Summary . . . 45
4.6 Tool Distributed Network Monitoring . . . 46
4.6.1 Ethical and Legal Aspects . . . 46
4.6.2 Technical Aspects . . . 48
4.6.3 Recommendation Summary . . . 49
4.7 Tool FERRET . . . 49
4.7.1 Ethical and Legal Aspects . . . 49
4.7.2 Technical Aspects . . . 51
4.7.3 Recommendation Summary . . . 51

5 Conclusions **53**

6 Annex **55**
6.1 Questionnaire A for Tool Developers . . . 55
6.2 Questionnaire B for Industrial Partners . . . 67

Nomenclature **74**

Abstract

Deliverable "D3.3 Legal and Architectural Feedback" describes some preliminary results gathered in the first period of WP3 *Validation support*. First we give an overview about the tools developed within CRISALIS. Based on the CRISALIS use cases, applicable laws and regulations and technical aspects, potential requirements to these tools are derived. Also ethical aspects are addressed. The implications of these requirements to each tool are analysed and recommendations for the tool developers are given in order to enhance the applicability of the tools for the later industrial usage.

1 Motivation and Scope

The tools developed within CRISALIS shall be as broadly applicable as possible. Therefore, conformance with laws and regulations and ethical requirements is essential. Examples are privacy laws, export restrictions and dual use aspects. Moreover, technical aspects originating from development, commissioning, and operational processes have to be considered. For usage of any tool within critical infrastructures, safety of persons, machines, and environment has highest importance.

The following analysis of the tools is based on the respective current development status.

In chapter 2 we present an overview of the tools and their properties. Chapter 3 refers to the CRISALIS use cases detailed in CRISALIS deliverable "D2.2 Final requirement definition" [12] and we derive ethical and legal requirements from relevant laws and regulations. In addition, technical and usability apects for tool usage are described. In chapter 4 these requirements are applied to each tool and respective recommendations are derived to be aware of legal and architectural contraints. Chapter 5 summarizes the given recommendations.

2 Properties of Developed Crisalis Tools

In this chapter, we give a short overview of the tools

- Avatar (firmware analysis),
- Access Miner (hypervisor),
- Smart Fuzzers (protocol fuzzers),
- FCScan (file and data scanner),
- Flow Fingerprinter,
- Distributed Network Monitoring, and
- FERRET (forensics)

developed within CRISALIS, their functioning and main properties which are required for the applicability analysis in the next chapter. For more details see the respective other CRISALIS deliverables as noted.

2.1 Tool Avatar

Avatar is an event-based arbitration framework that orchestrates the communication between an emulator and a target physical device. Avatar's goal is to enable complex dynamic analysis of embedded firmware in order to assist in a wide range of security-related activities.

The modular architecture lets Avatar perform dynamic analysis of firmware behavior, such as recording and sandboxing memory accesses, performing live migration of subroutines, symbolically executing specific portion of code as well as detecting vulnerabilities.

For a more detailed description see chapter 4 of CRISALIS deliverable "D5.3 Report on automated vulnerability discovery techniques" [7].

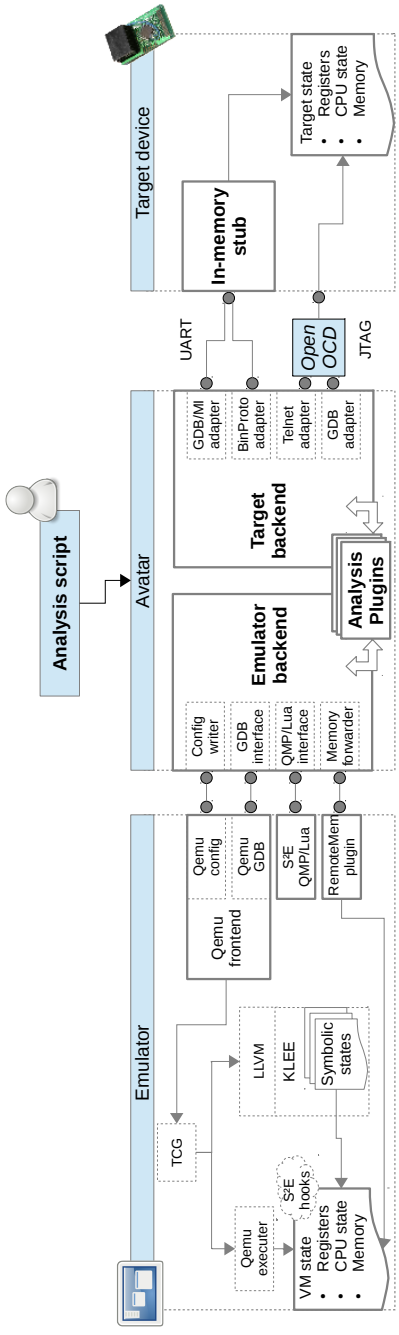

Figure 2.1: Overview of tool Avatar

2.2 Tool Access Miner

Access Miner is a host-based behavioral malware detector. It is designed to model the general interactions between benign programs and the underlying operating system (OS). In this way, Access Miner is able to capture which, and how, OS resources are used by normal applications and to detect anomalous behavior in realtime.

Access Miner is implemented as a custom hypervisor, which includes three sub-components:

Syscall Interceptor is designed to intercept the operations performed by the OS, in terms of system call type, parameters and return values. In order to retrieve all system call information, it monitors the invocation of the operation along with its own termination by hooking the sysenter instruction. Before passing the information to the Policy Matcher, the system also needs to check whether the operation is successful or not and to collect its return value. For this purpose, our hypervisor is able to intercept a sysexit instruction.

Policy Matcher: The goal of this component is to check Access Miner policies and to generate an alert in case some of them are violated. We recognize two main phases for the Policies Checker task: Initialization and Detection phase. The initialization phase is responsible to create the memory structures that will be used for the detection phase. In particular, to check the filesystem and registry policies, we adopt an hash table memory structure where the name of each resource is used as key and the name of process with its own permissions on that resource is stored as value. During the initialization phase, the hypervisor receives the signatures using the ad-hoc network communication protocol we briefly mentioned above. Then, whenever a signature is loaded, the full pathname of the corresponding resource is extracted and inserted in the memory structure as a key of the hash table. The list of the processes that can get access to the resource along with their own access permission are inserted as elements of such a key.

Process Revealer: The goal of this component is twofold: First, it extracts and provides the name of the process that is performing the actual operation (i.e., a system call) through Virtual Machine Introspection and, second, it caches this information to reduce the system overhead. The component keeps a cache that allows to lookup the name of the process given a certain CR3 value. The cache is updated every time a process is created or destroyed, by properly intercepting and analyzing process-related system calls.

For more information see chapter 2 of CRISALIS deliverable "D7.2 Preliminary report on host-based compromise detection" [8].

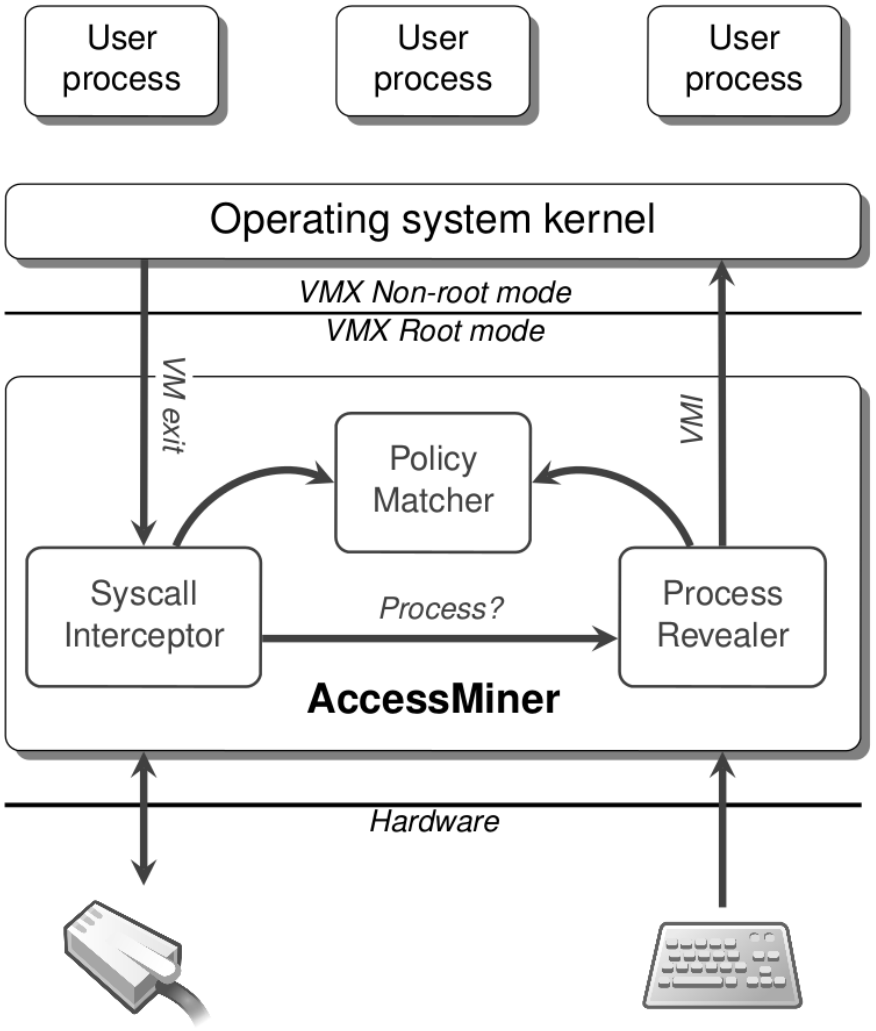

Figure 2.2: Overview of tool Access Miner

2.3 Toolset Smart Fuzzers

The toolset Smart Fuzzers allows testing the robustness of ICS protocol implementations for a number of popular ICS and AMI protocols.

Smart Fuzzers is implemented on top of the Peach framework. Each fuzzer consists of an XML configuration data file (a so-called Pit file). A Pit file is organized into Data models, State models and Test definitions. Data models define the format of protocol messages to be fuzzed. State models define the set of actions that the fuzzer needs to carry out for each test case (e.g., connect, send fuzz data for message X, disconnect). Tests tie together Data and State models and allows to configure test logging and a monitor allowing the fuzzer to detect if the System Under Test (SUT) is responsive after every test case.

To this end, the Peach framework was extended with a custom Valid Case Instrumentation monitor, which allows to remotely test if the SUT is responsive after every test case by checking if it is possible to connect to the fuzzed service and by using protocol-specific probing messages to check that the SUT is still operating as expected.

In a typical scenario, the Smart Fuzzers toolset is installed in a computer connected through the network to the device or application to test (the SUT). The toolset is run in batch mode, it executes a number of tests against the SUT and reports if faults were detected. For each supported protocol different test suites are available, corresponding to the different protocol messages to be tested.

For a more detailed description see chapter 3 of CRISALIS deliverable "D5.3 Report on automated vulnerability discovery techniques" [7].

2.4 Tool FCScan

FCScan is a passive monitoring tool that aims at detecting malicious electronic documents such as PDFs, Microsoft Office documents, engineering project files etc. FCScan first builds models of legitimate behavior by analyzing a number of benign samples, and then can be put into monitoring mode and flagging those documents that do not exhibit the same behavior.

For a more detailed description see chapter 3 of CRISALIS deliverable "D7.2 Preliminary report on host-based compromise detection" [8].

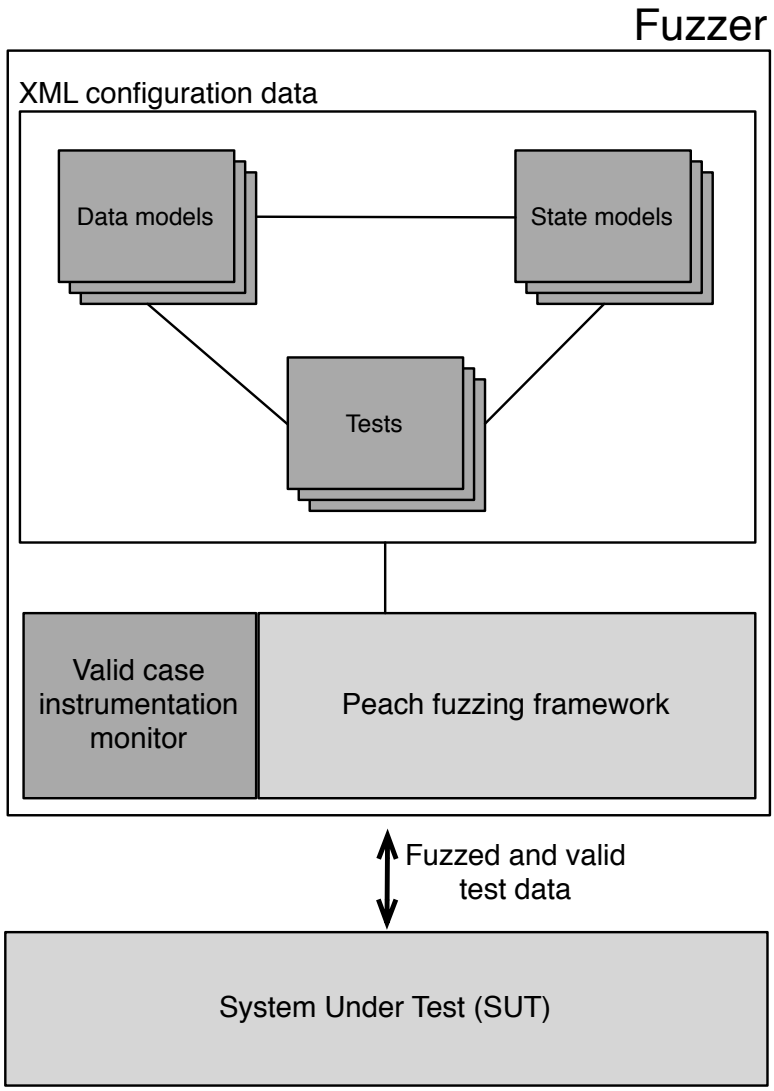

Figure 2.3: Overview of toolset Smart Fuzzers

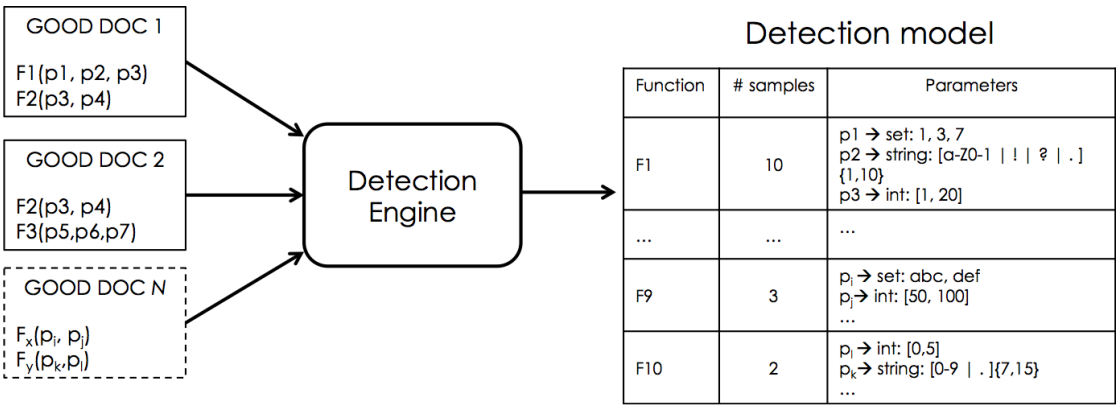

Figure 2.4: Overview of tool FCScan

2.5 Tool Flow Fingerprinter

Flow Fingerprinter (FF) is a passive fingerprinting tool that aims at recognizing ICS devices by looking at the generated traffic. The tool focuses on connections and communication patterns and creates a representation of the infrastructure under observation. FF relies on the hypothesis that "similar" ICS systems and components generate similar representations. Therefore it uses information about known devices, stored in a dataset, to recognize new ones.

The prototype monitors broadcast and multicast traffic that is delivered to the monitoring device. It decodes elements of the packets from a number of different protocols. The most important ones are:

- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)
- NetBIOS Name Discovery (NBNS)
- Simple Service Discovery Protocol (SSDP)
- Bonjour and LLMNR
- Switch protocols:
  - Spanning Tree Protocol (STP)
  - Cisco Discovery Protocol (CDP)

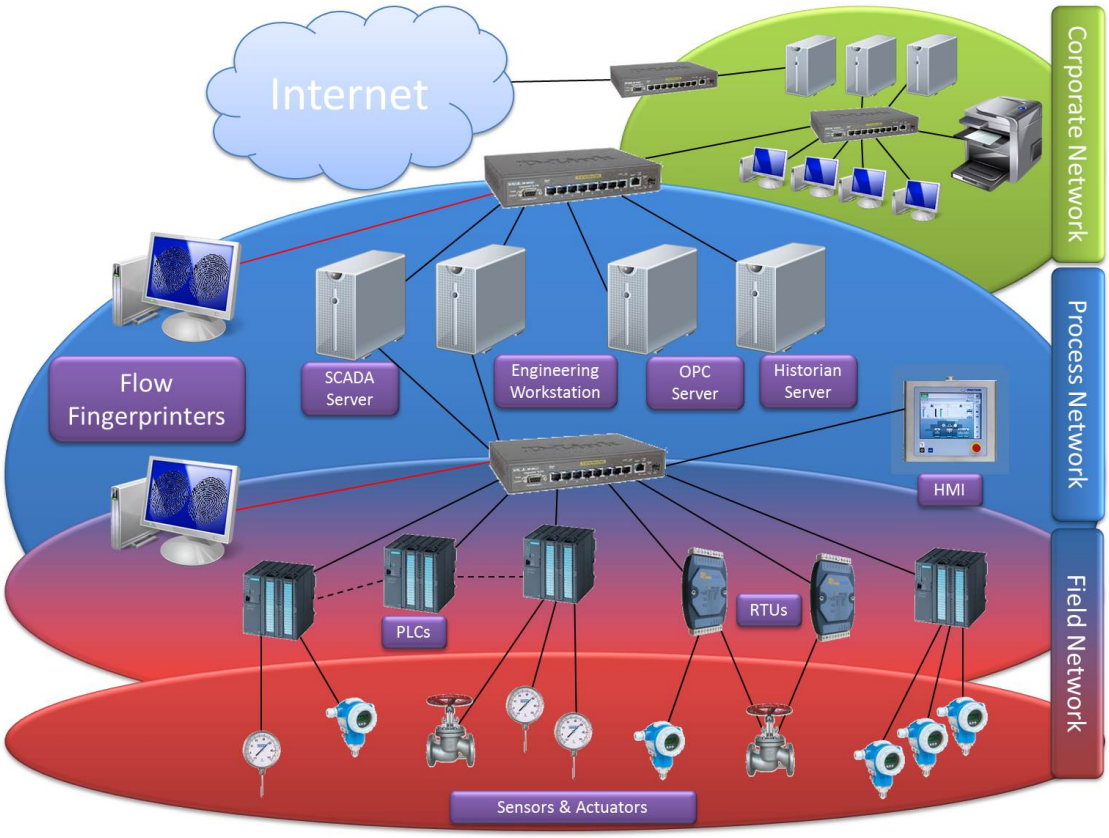

Figure 2.5: Standard setup of Flow Fingerprinter within a plant network

– Link Layer Discovery Protocol (LLDP)

A more detailed description can be found in CRISALIS deliverable "D4.4 Device Fingerprinting" [10].

2.6 Tool Distributed Network Monitoring

The purpose of the interaction modelling tool is to passively provide information on the state of the network by monitoring which devices are/were connected and how these devices are connected in terms of the types of messages they exchange. By applying protocol learning we derive templates of messages which allow us to assign labels to packets exchanged between two systems. Ideally the goal here is to assign the same label to similar messages exchanged between different pairs of hosts. In conjunction with device fingerprinting this allows building a profile of a particular operations of a device by looking at its communication patterns and partners. This in turn allows us to understand the network better without requiring a priori knowledge of the underlying systems and also serves as the basis for the intrusion detection tool that was scheduled for next year.

The tool in its current state is an offline tool, it requires as inputs network pcap traces which are then parsed. The final goal was to have a system where we have lightweight access points on each network segment. This could either be via network taps or by using small systems such as raspberry pi's that collect the information. Since its passively gathering data it has no impact on its environment, beyond the need for the multiple devices aggregate the collected PCAP traces. The tool takes usually a few minutes to run and parse a 100 MB PCAP file containing a particular protocol plus the time needed to apply protocol learning, which varies depending on the protocol but should take less then 15 minutes.

On a component level the tool is separated aside from capturing network traffic the system is composed into three logical components, a portion that parses the PCAP files into something thats easier to manage, a protocol learning component that generates a system for labelling individual messages and a graphing component that aggregates information from packets and their labelling to generate an overview of the layout of the network.

For more information see CRISALIS deliverable "D6.2 Protocol-agnostic approaches" [11].

2.7 Tool FERRET

FERRET is a tool for forensic data analysis of Windows computers which are used in automation control systems (control centers, engineering station, operator station, etc.).

FERRET consists of an agent which can be run on these machines in case of suspected malware infection or other strange behaviour, and gathers data required for forensic analysis. The second part of FERRET is an automated processing system at the forensic expert's site which enriches the data with forensic analysis knowledge.

Before any data collection can take place, required permissions of system owner and manufacturer has to be obtained. It is useful to make two "snapshots" of the system (one at first start up and another one sometimes later during operation, but before any infection) to determine the "ground state" and the "drift" of the system. This allows much easier detection of changed parameters, e.g. new registry entries caused by malware.

The bulk of data (about 100 GB) on the machine is not collected, just some metadata and few executables (about 100 MB):

- filesystem
- configuration / Registry on Windows
- runtime date (Processes, Connections)
- logfiles (events, antivirus, FW, etc.)
- certain executables

These data are transmitted via a secure SSH connection to the forensic expert's site; if there is no such connection possible, an operator or service technician may send the data by other means (e.g. E-Mail or ftp).

At the forensic expert's site, the data are automatically processed by

- converting data to ASCII or machine readable xml,
- augmenting with data from external databases, and
- interpreting data

Then, the forensic analyst reviews the processed data regarding

- malware detected (score)
- universal timeline (one large timeline of all events)

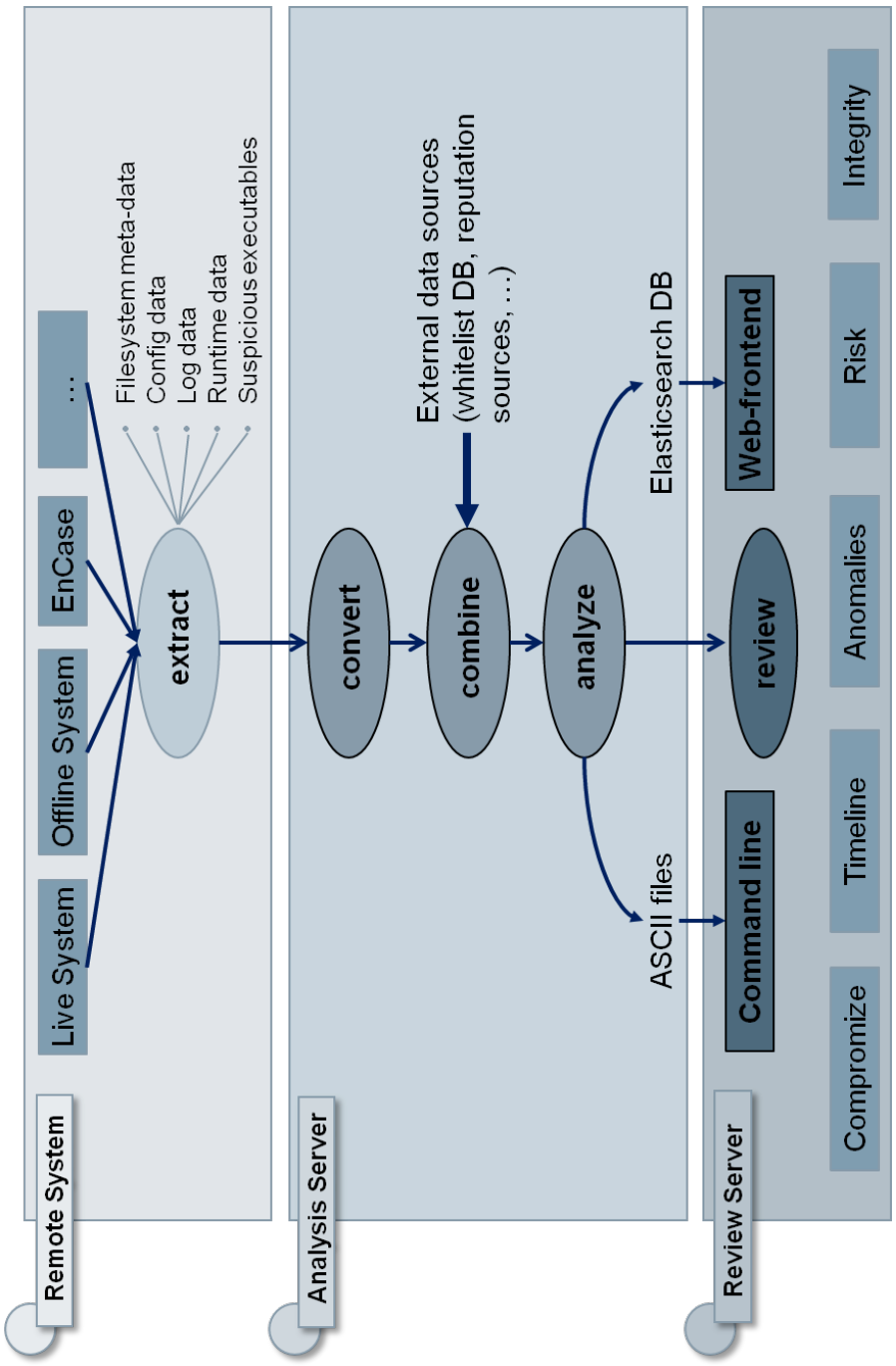

Figure 2.6: Components and workflow of tool FERRET

- review of logfiles from runtime data
- remaining risk on that component (e.g. unpatched software)

and gives the operator hints how to proceed further with the machine (e.g. no infection found, or clean some files, or reinstall the machine).

A more detailed description will be available in CRISALIS deliverable "D7.3 Report on forensic analysis for industrial systems" [13] in November 2014.

3 Use Cases and Requirements

3.1 Use Cases

For analysing the practical applicability of the tools developed in CRISALIS, we focus on our two use cases:

1. distributed control system (DCS) of a power plant (see section 3.1 of [12]) and
2. advanced metering infrastructure (AMI) for gathering data from electricity (and gas and water) meters (see section 3.2 of [12]).

Because the power plant DCS is very typical for automation systems in many areas of industrial automation (such as chemical plants, pipelines, food production, pharmaceutical plants, etc.), this provides a comprehensive evaluation of the tools.

The applicability depends on the phase of development and operation when the tool shall be used. We evaluate the applicability therefore according to the following "life cycle phases" of plant or system operation (including AMI):

- component design and development
- component test
- integration of components into a solution or system
- test of integrated solution
- comissioning of plant, field test of smart meters
- start-up of active plant or system
- operation of active plant or system
- shut-down of active plant or system
- maintenance of plant or system
- offline analysis of a component (e.g. firmware, protocol stack) in a test lab

- offline analysis of recorded data from the plant (e.g. network traffic)
- offline analysis of recorded data from plant components (logfiles, memory dumps)

The requirements in the following sections are compiled based on the knowledge from the industrial project partners. A first input was gathered by using questionnaires (see Questionnaire B in section 6.2), and deepened in a workshop.

3.2 Requirements

3.2.1 Ethical and Legal Requirements

Remark: As we are no legal experts, our legal evaluation is based on our layman knowledge and interpretation of laws and regulations which may be incomplete and inaccurate. Therefore, this analysis cannot replace an evaluation by lawyers, but just indicates potential problems and solutions which have to be investigated by lawyers in more detail.

The ethical aspects of the FP7 framework ethics checklist [6] which are relevant for Crisalis are "Privacy" and "Dual Use". Furthermore, we address some additional legal aspects so that the total list of addressed aspects looks like this:

- Privacy
- Dual Use
- Warranty
- Defects Liability
- Trade and Usage Restrictions
- Intellectual Property Rights
- Further Legal Aspects

Privacy

In modern democracies, data protection laws only emerged a few decades ago, aiming at protecting information on private individuals from intentional or unintentional disclosure or misuse. Through the increasing use of automated data processing and online communication, the collection and correlation of data gets easier and easier. Data protection is necessary to protect personal data, like for example customer identification

data, consumption profiles, employee data, etc. from being revealed for purposes other than originally intended. The term "personal data" is defined in the Directive 95/46/EC on Protection of Personal Data [1] as *"any information relating to an identified or identifiable natural person [...]"* (art. 2(a)). Most member states provide definitions in this sense, e.g.:

- The German Federal Data Protection Act (BDSG) [3] defines personal data as *"any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)"* (§3)

- The Dutch Personal Data Protection Act [2] also defines personal data as *"any information relating to an identified or identifiable natural person"* (art. 1 (a)).

Though, a few countries extend the scope like e.g. Italy: the Italian Personal Data Protection Code [4] additionally covers data of legal persons (e.g. company name, address ...): *"any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number"* (section 4, §1 b)).

Accordingly to these definitions, two types of personal data may likely be processed in DCS and AMI, respectively:

- Times of login, work actions, and logout of operator personnel. This may be used to monitor employee activity (only DCS).

- Metering data. Consumption data of electric power, gas, and water make comprehensive behaviour analysis of end customers possible (only AMI).

The handling of such personal data is subject to legal privacy requirements related to legitimacy, transparency, and proportionality, which may though differ slightly from one EU member state to the other, as described below.

Legitimacy: According to the European Directive 95/46/EC on Protection of Personal Data, personal data shall be collected and processed only for the specified, explicit and legitimate purposes (art. 6 1(b)). This requirement is stated as a principle of the German BDSG (§14, §31, §39), the Italian Personal Data Protection Code (§11), and the Dutch Personal Data Protection Act (art. 7). This implies that an explicit consent of the data subjects (e.g. customer, employee) or another means of justification (e.g. contract) is required with respect to the use of his personal information (e.g. meter data, employee data) for the given purpose. Some countries like Germany and Italy additionally require the data subjects consent in written form. Thus, relying on implied

consent by displaying an information message upon login would not be enough to justify employee monitoring in DCS.

Transparency: The European Directive 95/46/EC on Protection of Personal Data requires that EU Member States transpose the following transparency requirements into compliant national laws, when processing personal data:

- The data subject (e.g. consumer, employee) should have a clear understanding which data is collected and how it is processed and used.
- The data subject has to be notified about the processing of his personal data.
- The instance responsible for the processing of personal data (i.e. data controller) must provide its name and address, the purpose of processing, the recipients of the data and all other information required to ensure a fair processing.
- Access to data has to be granted to the data subject. There must be a way for customers to find out which personal data is stored for the stated purpose and how it is used.
- Data must be rectified, erased, or blocked if wished by the data subject. This implies that there must be a way for end customers or employees to correct their personal data and to opt out at any time. In such a case, their personal data must be securely deleted. If erasure is not possible, a functionality to lock data must be provided.

Corresponding requirements can be found in:

- the German BDSG in §19 (access to data), §19a (notification), §20 (rectification, erasure and blocking of data; right to object);
- the Italian Personal Data Protection Code in §7 (right to access personal data and other rights);
- the Dutch Personal Data Protection Act in art. 27-28 (notification), art. 35 (access to data), art. 36 (rectification, erasure and blocking of data), art. 40 (right to object).

Moreover, notification of data protection authorities might be necessary in different forms according to the country:

- In Germany, only the notification of an appointed data protection officer is required (see BDSG §4d "obligation to notify"), who shall then in turn inform the Federal Commissioner for Data Protection and Freedom of Information if he has got any doubts that the data processing is not adequate.

- The Italian Personal Data Protection Code requires the notification of data processing if it concerns, for example: *"data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users"* (§37, 1.d). This notification shall be addressed to the Italian Data Protection Authority ("Garante") in electronic and digitally signed form prior to starting the processing, but also in case of modifications and at the end of processing. The personal data handled in DCS clearly fall under the category of data for which notification is required in Italy.

- Article 27 of the Dutch Personal Data Protection Act requires the notification of the Data Protection Commission or to an appointed data protection officer, prior to processing. This notification is relevant if CRISALIS tools process personal data in AMI.

Proportionality: The European Directive 95/46/EC on Protection of Personal Data requires that processing of personal data is performed in accordance with the following proportionality requirements:

- Data processing must be adequate, relevant and not excessive in relation to the purposes for which data is collected and/or further processed. This implies that data shall be anonymized or at least pseudonymized when the connection to the person is not required for processing purposes. This has to be checked for the tools developed within Crisalis.

- Personal data shall not be disclosed to third parties unless authorized by law or by consent of the individual.

- Data has to be kept accurate and up to date.

- Adequate data processing must include protection against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

In Germany, the Annex to BDSG §9 (1) requires the following protection measures:

- Access control (to prevent unauthorized access to and usage of systems processing or using personal data and to prevent access to personal data, except as defined in the access control model)
- Disclosure control (to prevent unauthorized operations on personal data during transmission, transport or storage, and ensure the control of correct distribution of data)
- Input control (to ensure that it can be detected afterwards whether and by whom personal data were inserted, changed or removed)
- Job control (to ensure that personal data processed on behalf of others are processed only in the way they were ordered to)
- Availability control (to protect personal data against accidental loss or destruction)
- Separation of processing (to ensure that data collected for different purposes are processed separately)

Finally, state-of-the-art encryption is explicitly stated as an appropriate measure for protecting access to personal data.

The Italian Personal Data Protection Code (§34 and Annex B) also specifies minimal security measures to be adopted:

- Access control (user authentication based on user IDs and passwords, authorisation system)
- Documentation control:
  - Regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means
  - Up-to-date documentation on the protection measures in the form of a security policy document
- System hardening (protection of electronic means and data against unlawful data processing operations, unauthorized access and specific software)
- Availability control (by implementing procedures for safekeeping backup copies and restoring data and system availability).

Finally, if public agencies are involved, further state / regional laws might be relevant. For example, in Germany, state data protection acts regulate the handling of personal data about individuals in state administration and public agencies.

Whether the tools developed within the Crisalis project handle personal data and must thus fulfill the above-mentioned requirements will be examined for each tool in section 4.

Dual Use

This means the illegal usage of the tools by adversaries like foreign military and terrorists to threaten or attack critical infrastructures. We also include "black hat hackers" and criminals.

Even totally defensive tools may be used by foreign military and agencies to enhance the protection of their IT systems, or to analyze security events. However, we cannot judge the resulting consequences.

Warranty

Certain actions during the usage of the tools (e.g. opening of the chassis) may invalidate the warranty of components given by the manufacturer, or the warranty of the integrated solution or system given by the integrator.

Defects Liability

Responsibility of the tool developer for correct functioning of the tool.

Trade and Usage Restrictions

Restrictions to export, import or use goods within a country. IT Security (see section 5.A.2 of [5]) is a topic of the Wassenaar export restriction list for dual use goods. This may restrict or prevent distribution of developed Crisalis tools outside of the EU.

The tools may contain technology and software with US origin (e.g. developed within the US or by US citizens). If this parts exceed 10% of the total product, the tool is subject to US export regulation.

The anti-hacking clause of the German Criminal Code (Anti-Hacker-Paragraph: §202c Strafgesetzbuch (StGB)) prohibits development and distribution of hacker tools in case of preparation of illegal hacking (§§202a, 202b StGB). Although developing, getting and using such tools for benevolent hacking (penetration testing explicitly authorized by the

system owner) is not intended to be illegal, some security experts see there a “legal limbo”.

In The Netherlands, usage of tool for penetration testing must be restricted to systems that the user owns or to systems that she has explicit permission to use. All other use is considered “computervredebreuk” under Dutch law “Wetboek van Strafrecht art. 138ab” and can lead to fines or jail sentences.

Intellectual Property Rights

Usage of the tool may violate Intellectual Property Rights of manufacturer, solution provider (integrator) or other third parties. We do not investigate potential violation of IPR by the tool’s technology because it is good practice that tool developers investigate on existing state of the art technology and patents upfront.

IPR restrictions may also include the prohibition of Reverse Engineering.

Further Legal or Ethical Aspects

All further legal aspects which are not already covered by the topics above.

3.2.2 Technical Requirements

For the analysis of the technical requirements, we focus on the following aspects:

Safety

Usage of the tool must never affect the safety of the plant or system!

System Requirements

The tool may require certain system conditions, e.g. used traffic bandwidth, free memory on components etc.

Performance

The tool may affect system performance.

3.2.3 Usability Requirements

Applicability of tools strongly depends also on usability aspects. Here we provide several usibility requirements which shall be kept in mind during the tool development.

However, CRISALIS is a research project and not meant for developing a finished product. Therefore, these topics are out of scope for CRISALIS so we do not discuss these topics in relation to specific tools in the next chapter.

Required Technical Skills of Intended Tool Users

The tool developers should have in mind the expected technical skill of their target group of tool users. Operators in a plant, maintenance technicians, etc. usually have a deep knowledge in their respective domain, but are no experts of IT technology or security. Therefore, the tools should be easy to use even for non-experts. An intuitive user interface and a good documentation is important.

Effort of Tool Usage

The effort for installation, operation and maintenance of the tools should be low to make the tool attractive, especially for people who try the tool for the first time. Getting updates must be easy, or even automated.

Integration with Other Tools

Good applicability may require an integration of the tool into other, already existing tools, e.g. control center of the plant, or the engineering station.

Long Time Support

Device manufacturers and solution providers require long-term support (hardware and software maintenance) for all used components. Components without such a support may not be usable for professional operation. Especially if a tool is provided as part of a more comprehensive solution, e.g. part of a turn-key solution for plant automation, guaranteed long time support is essential.

4 Applicability Analysis

Here we analyze the tools from section 2 according to the requirements from section 3.2.

4.1 Tool Avatar

The Avatar tool is designed to perform emulation and sophisticated dynamic analysis task on the firmware of embedded systems. Avatar is *not* an automated vulnerability discovery or reverse engineering tool.

In the context of the Crisalis project, it has three main use cases:

1. Analyze modified and (potentially) malicious firmwares.
2. Discover vulnerabilities in firmwares.
3. Support the fuzzing process to understand the consequences of certain inputs.

Avatar can be used during component development and test, and also to analyze components in a test lab. For reasons explained below, Avatar must never be used on safety-critical components in operation! Neither must analyzed devices be put back in an operational system.

4.1.1 Ethical and Legal Aspects

Privacy

Avatar is a tool for analyzing firmware of embedded devices. During this process, the tool gains access to the device memory.

Depending on device type and history, privacy relevant data may be stored on the device. For instance a smart meter (but also e.g. a medical personal monitor or a digital tachograph) may contain privacy relevant data after having been in operational use. The investigator using Avatar to analyze the device may not be entitled to view these data due to privacy restrictions.

Therefore, prior to the analysis of a device which has already been in operational use, the end user shall be informed that an analysis with Avatar might disclose personal data

to the investigator using the tool (e.g. consumption profiles in smart meters), and end user's consent to this investigation shall be documented in written form.

These restrictions do not apply for analysis of devices which have never been in operational use, and devices which memory was erased in a way so that privacy related data can not be contained anymore.

Furthermore, we recommend that written user documentation of Avatar as well as in-operation user guidance of Avatar (e.g. the splash / welcome message) should contain a clear caution regarding the potential infringement of user privacy when analyzing a device which has already been in operational use. It should be part of Avatar's usage policy to obtain counseling from the privacy protection officer in charge before using it on such devices.

Dual Use

Avatar allows for dynamic analysis of device embedded firmware behavior. Legitimate device producers and mostly device owners may use the tool to find vulnerabilities and malicious modifications.

Avatar is an emulation tool, and not an automated reverse engineering tool. However, attackers who can get an embedded device may abuse Avatar to become familiar with the firmware. Avatar can be used to retrieve static information and behavior in operation, and to analyze location of and reason for patches. This may help attackers to detect new vulnerabilities to abuse and to locate known vulnerabilities in other devices with similar firmware for which a patch is not yet available from the manufacturer. The latter effect is well-known from reverse-engineering patches in operating systems. Avatar can be misused for reverse-engineering of firmware, which may be abused by attackers both to infringe intellectual property rights and to write malware and malicious "patches" for the firmware.

This is true for most of static and dynamic analysis tools, such as system emulators, debuggers, disassemblers, etc. However, since Avatar requires physical access to the embedded device and opening of the device to install a backend adapter, it seems unlikely that the tool can be used unauthorized in a productive environment without being noticed.

Warranty

As Avatar requires opening of the device to install a backend adapter, this may void the warranty of the device. The device owners consent must be obtained before tampering with the device.

Furthermore, the device may be severely damaged.

Defects Liability

Avatar is an interactive tool. The detection of malicious firmware modifications and vulnerabilities strongly depends on the skills of the investigators as well as on the quality of the tool and firmware. So neither the tool nor its developers can guarantee that all existing vulnerabilities or malicious modifications are found (no false negatives), and that no findings are interpreted wrong (no false positives). This is obvious for a skilled expert, but anyway an explicit warning should be added to the usual software disclaimer (like "This software is provided as it is " which often comes with free software) to protect the tool developers from legal responsibility.

Trade and Usage Restrictions

Avatar is being developed in France. It does not use cryptographic or cryptoanalytic functions. We see therefore no reason for Avatar being subject due to EU export regulation (based on the Wassenaar agreement list for dual use goods).

If the share of software with US origin exceeds 10%, the tool may nevertheless be subject to the US export regulation.

(Attempts to) Reverse engineering may be prohibited by law in certain countries. This may especially be true if the firmware has been code obfuscated, as then a technical control would need to be circumvented as well, which at least in the context to digital rights management may be illegal in several countries.

The German Anti-Hacking law forbids creation, provision and distribution of tools whose primary purpose is hacking. However, invited penetration tests with consent of the operator are permitted. In the case of Avatar consent of the device manufacturer may also be required.

Intellectual Property Rights

Analysis of firmware with the explicit goal of reverse engineering may infringe intellectual property rights. If Avatar is used to support the reverse engineering of a Firmware, and depending on the country in which the operation is performed, a permission of the device or firmware manufacturer may be required. A caution in the user documentation should warn the user to ensure the lawfulness by getting a permission of the device or firmware manufacturer first before of analyzing a given firmware or device.

Further Legal or Ethical Aspects

Vulnerabilities found with the help of Avatar must be treated with high responsibility, for instance by allowing the device manufacture time to patch the vulnerability before disclosing it to the general public. For a discussion of "responsible disclosure" see chapter 6 of CRISALIS deliverable "D5.1 Security Testing Methodology", version 2 [9].

4.1.2 Technical Aspects

Safety

Avatar interacts with the firmware of the device and may (depending on the device communication ports) require dismantling of the device. This may adversely affect the reliability (and performance) of the device, and the safety of the DCS. Therefore, Avatar must never be deployed on safety-critical components during operational phases of an active plant or system!

Furthermore, because using Avatar may damage the device or change firmware or configuration, an analysed device shall never be put back into service in an operational plant or system.

Opening the device chassis and running Avatar on a dismantled device may expose the tool user to personal danger, danger of e.g. electric shock by not isolated wires.

System Requirements

Avatar requires dismantling of the device, that means opening the chassis. It requires installation of a special backend adapter in the opened device, interaction with the running firmware and r/w access to the memory of the device (like via a JTAG or serial interface). Supported interfaces should be described in the tool documentation.

Currently, Avatar supports ARM or x86 architectures only. The user documentation should state which sub-versions of these two processor types Avatar has successfully been used with.

Performance

Avatar being an interactive tool, so it does not in itself seem likely to suffer from grave performance issues.

But the performance of the investigated device may be reduced, so real time requirements may be violated (see section Safety).

4.1.3 Recommendation Summary

To further enhance to applicability of Avatar, we recommend to consider the following measures:

- Put a warning into the user manual that the tool must never be used on safety critical components in operating plants.
- Put a warning into the user manual that the tool user shall be obey safety hints of the device's manual when opening the chassis.
- Put a warning into the user manual that opening the chassis may void the warranty.
- Put a warning into the user manual that the device may become damaged and that it must never be put back in a safety critical, operational environment.
- Put a standard software disclaimer in the manual and the source code.
- Put a warning into the user manual that device owner's permission is required.
- Put a warning into the user manual that device manufacturer's permission may be required.
- Put a warning into the user manual that personal data may be disclosed.
- Get the informed consent of end users in written form when getting devices for analysis which may contain personal data.
- Get counseling from the privacy protection officer in charge for the Avatar analysis purposes.
- Support the most common processor types of embedded devices.
- Support the most common (suitable) interfaces of embedded devices.
- Clarify share (percentage) of potentially contained US software, e.g. of included Open Source Software libraries.
- Get approval for distribution (export) by legal department.

4.2 Tool Access Miner

4.2.1 Ethical and Legal Aspects

Privacy

AccessMiner only intercepts system calls without storing their content. This operation does not involve privacy-related data. Therefore, the privacy topic is not relevant for Access Miner.

Dual Use

AccessMiner is used to detect anomalous operations performed by software installed in the machine. If properly tuned, these operations are typically associated to malicious software running on the computer. AccessMiner cannot be used to find vulnerabilities. Therefore, it is of no use for hackers, and we do not regard it as dual use tool.

Warranty

Installing additional software may void the warranty of a device or a component.

Defects Liability

The tool provides has either to guarantee the absence of flaws in the tool by comprehensive testing and certification, especially if it is intended to be used on safety critical components during operation, or to explicitly declare that the tool must not be used if component's owner / operator is not willing to bear that risk on her own.

Trade and Usage Restrictions

We see no reason for Access Miner being subject due to EU export regulation (based on the Wassenaar agreement list for dual use goods).

If the share of software with US origin exceeds 10%, the tool may nevertheless be subject to the US export regulation.

Intellectual Property Rights

AccessMiner does not perform any analysis of software, but it only observes the external behavior of a program in the way it interacts with the underlying operating system. Therefore we do not believe that AccessMiner could be used to infringe intellectual property rights.

Further Legal or Ethical Aspects

As AccessMiner cannot be used to find vulnerabilities, we do not foresee any additional legal or ethical aspect.

4.2.2 Technical Aspects

Safety

For usage in safety critical components during operation, freedom of any side effects has to be provided. Furthermore, certification may be required.

Access Miner may be used in not safety critical components without restriction, even during operation.

System Requirements

None.

Performance

A reduction of computation speed is expected when the system is protected by Access-Miner

4.2.3 Recommendation Summary

To further enhance to applicability of Access Miner, we recommend to consider the following measures:

- Put a warning into the user manual whether the tool may be used on safety critical components in operating plants.
- Put a warning into the user manual that installation of additional software may void the warranty.
- Put a warning into the user manual that the device may become damaged and that it must never be put back in a safety critical, operational environment.
- Put a warning into the user manual that device owner's permission is required.
- Put a warning into the user manual that device manufacturer's permission may be required.

- Put a standard software disclaimer in the manual and the source code.
- Clarify share (percentage) of contained US software, e.g. of included Open Source Software libraries.
- Get approval for distribution (export) by legal department.

4.3 Toolset Smart Fuzzers

Smart Fuzzers can be used during component development and test, and also to analyse components in a test lab. It may be used for devices, and for pure software applications running on a host machine.

For reasons explained below, Smart Fuzzers must never be used on components in an operation plant or system! Neither must analysed devices be put back in an operational system. Smart Fuzzers must also not be used within the communication network of an operating plant or system.

4.3.1 Ethical and Legal Aspects

Privacy

Smart Fuzzers does neither record nor process any privacy relevant data: It just sends packets to the targets which may not be compliant to the used protocol or application standard, and observes the reaction of the target. It does not read out data (e.g. configuration or log data) from the target, and may therefore be used without restrictions even with devices which contain some potentially privacy related data.

Dual Use

The goal of fuzzing or fuzz testing is to verify and enhance the robustness of the implementation of a target product (device or application) in handling abnormal input data. Automated Fuzzing complements human testing by providing further test cases, and achieves results that cannot be achieved by human testers.

On the other hand, implementation weaknesses found using fuzz testing may be exploitable vulnerabilities that could be used by a real attacker. Additionally, a fuzzer may be used directly as a DoS attack tool or to find new DoS attacks. Therefore, we consider Smart Fuzzer as a potential dual use tool.

Warranty

Toolset Smart Fuzzers works via network, so opening of the device is not required.

Usually, fuzz testing may cause a device at worst to "hang up", so that a reboot (e.g. by disconnecting the power supply) and maybe even a new configuration after factory-reset is required. In the test, a device was physically damaged by the fuzz testing so that it hab to be replaced. We don't see that fuzz testing may invalidate the warranty of the device because in a real operational environment the device may receive such messages from an attacker, and it has to be so robust that even a hang up does not occur.

Defects Liability

Smart Fuzzers must never be used in an operating plant (see section Safety) because may crash or even severly damage a device! The tool developer has to clearly state this in the user documentation to avoid responsibility.

Trade and Usage Restrictions

We see no reasons for Smart Fuzzers to be subject to the Wassenaar export control list.

Smart Fuzzers requires installing the Peach fuzzing framework, which is developed and distributed free of charge by DejaVu Security, an US-based company. If the share of components (Peach and maybe others) which was developed within the US or by US citizens exceeds 10% of the total product, the whole software is subject of the US export control regulation. Because Smart Fuzzers is a tool for development and test, we expect that it will be mainly used only in the countries where the development and test labs of device manufacturers are, but not on-site worldwide. Therefore, even potential restrictions due to the US export regulation may not significantly harm the usefulness of Smart Fuzzer.

German anti-hacking regulation (§202c of German Criminal Code) forbids the creation, provision and distribution of tools which are destined for hacking. However, "friendly hacking" (penetration testing) with explicit consent of the system owner is allowed. Because of possible usefulness also for attackers, Smart Fuzzers may be within a "grey zone".

Usage of the Smart Fuzzers must be restricted to systems that the user owns or to systems that she has explicit permission to use. Smart Fuzzers should be preferably used in a separate network with owned devices only; in case of remote testing the user has to make sure to scan only devices which she is authorized to.

Intellectual Property Rights

It is not clear to us whether fuzz testing may be regarded legally as reverse engineering. This has to be checked by a lawyer with detailed knowledge in that area.

Further Legal or Ethical Aspects

Vulnerabilities found with the help of Smart Fuzzer must be treated with high responsibility, for instance by allowing the device manufacture time to patch the vulnerability before disclosing it to the general public.

4.3.2 Technical Aspects

Safety

Smart Fuzzers is designed to be used by developers and test engineers during product and system development and test phases. Smart Fuzzers can crash running devices and applications, and therefore must never be used in a productive environment! The Smart Fuzzers developer has to warn the user not to use the tool in operational environment!

System Requirements

Smart Fuzzers focuses only on testing the "server" implementation of the protocols, i.e. the device or application that accepts incoming TCP connections.

At the moment, Smart Fuzzers supports the following popular ICS/AMI protocols:

- Modbus/TCP (ICS)
- OPC-DA (ICS)
- "PP" (ICS proprietary protocol form a major vendor)
- M-BUS (AMI)

Performance

After setting up the configuration, Smart Fuzzers runs without human interference and records the results. The total time may be estimated in dependence of the amount of test cases and the rate of test messages. However, occasionally a manual interaction may become necessary, e.g. to restart the device or push a factory reset button when Smart Fuzzers successfully detects a weakness in the target's implementation. This may strongly increase the time for successfully fuzzing a component.

4.3.3 Recommendation Summary

To further enhance to applicability of Smart Fuzzers, we recommend to consider the following measures:

- Do not make Smart Fuzzers available for everybody, especially not in Germany. License it only to people who have a verifiable interest in legitimate use (e.g. penetration testers, researchers).
- Put a warning into the user manual that the tool must never be used on safety critical components in operating systems.
- Put a warning into the user manual that permission of the component's (device, software application) manufacturer may be required.
- Put a warning into the user manual that the device may become damaged and that it must never be put back in a safety critical, operational environment.
- Put a standard software disclaimer in the manual and the source code.
- Support the most common DCS protocols.
- Clarify share of US software, e.g. of used Open Source Software libraries.
- Get approval for distribution (export) by company legal department.

4.4 Tool FCScan

4.4.1 Ethical and Legal Aspects

Privacy

FCScan analyses the behaviour of active documents and data to look for potential malware, similar to a virus scan program. It does not analyse nor store the documents content. Therefore, we see no privacy aspects here.

Dual Use

FCScan can only be used to detect potential malware. We see no dual use aspects here.

Warranty

Due to its passive nature, FCScan is not expected to affect the plant's network directly. But when installed on a component like a HMI server, it affects this component by using CPU time and memory. It may be installed even on safety critical servers but only before or during the certification process. An installation afterward may invalidate the warranty of the plant integrator and the operation permit given by the regualtory agency.

Defects Liability

Misidentifications of scanned data may result on false alarms, and blocking valid documents and engineering data which are required for system operation.

Trade and Usage Restrictions

FCScan is useful when deployed in already installed plants as well as in newly built ones. Worldwide on-site usage - and therefore the possibility to export it to foreign countries - is essential for a wide applicability of the tool.

FCScan may be regarded as system for detection of stealthy intrusion, but due to the exception note it is not subject to the Wassenaar regulation for export restriction:
5.A.2.a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
Note 5.A.2.a.8. applies only to physical layer security. [5]

FCScan may contain technology and software developed within the US or by US citizens. If this parts exceed 10% of the total product, it is subject to US export regulation.

Intellectual Property Rights

Scanning data with FCScan does not violate IPR of document or data owners.

FCScan does no reverse engineering which may violate reasonable usage restrictions.

Further Legal or Ethical Aspects

None.

4.4.2 Technical Aspects

Safety

FCScan may be used during all operation phases but certification may be required when used on safety critical components.

System Requirements

None.

Performance

It should be possible to be run in a separate process with low CPU priority to minimize potential performance degradation on critical components.

4.4.3 Recommendation Summary

To further enhance to applicability of FCScan, we recommend to consider the following measures:

- Put a warning into the user manual that permission of a certification agency may be required, especially when used on safety critical components.
- Put a standard software disclaimer in the manual and the source code.
- Provide detailed documentation and warnings about effects of potential misidentifications.
- Keep the percentage of software with U.S. origin low, well below the de minimis limit of 10%, to stay independent of U.S. export regulation. Provide the possibility of downloading further software as plug-in if necessary.
- Get approval for distribution (export) by company legal department.

4.5 Tool Flow Fingerprinter

4.5.1 Ethical and Legal Aspects

Privacy

Flow Fingerprinter (FF) identifies sending devices by investigating IP headers data, and comparing to a database of corresponding signatures. FF does not rely on message

content or store messages. Therefore, FF does not record, process or store privacy-related data.

Nevertheless, FF may identify special devices which are assigned to certain persons, e.g. a special service laptop, tablet or smartphone which is used in the plant for operation and control by one or few technicians only. On this basis, activity patterns of these persons may be detected with the help of FF if this assignment (personnel-equipment) is known. The possibility of analyzing such activity patterns with FF can be avoided by providing all plant technicians identical equipment (hardware and software), or by changing frequently the assignment of personnel and equipment in a randomly manner.

Anyway, as it is much easier to detect these activity patterns by using other network sniffers, e.g. by analysis of authentication requests and other authenticated messages, the use of FF only raises minor concerns related to privacy.

Dual Use

Flow Fingerprinter primarily does network analysis and is similar in effect to many network management tools. Such network monitoring tools are usually not considered dual-use.

Warranty

Due to its passive nature, Flow Fingerprinter is not expected to affect the plant's network in any way when it is deployed as separate hardware or only listening to wireless communication. When installed on a regular network component, it may affect this component by using CPU time and memory. Therefore, it should be preferredly be installed only on components which are not essential for the plant operation, especially not safety critical components.

Defects Liability

Misidentifications of components and their versions may have different effects:

- False positives: If there are a few misidentifications which claim that up-to-date devices are outdated, the operator may buy new ones and cause an minor but unnecessary financial loss. If there are many such misidentifications, the operator will check manually and will discover the false positives.

- False negatives: Outdated components which are not discovered can be a serious security issue. However, without this tool the plant operator may also not be aware

of outdated components. Therefore, only in the case when the plant operator neglects other organzisational measures (keeping a device and version directory) because he relies on this tool only, the network security may become worse.

- Misidentifications can cause also the operator to provide wrong updates to components. This may severely damage components if there is no protection mechanism by the component manufacturer.

Trade and Usage Restrictions

Flow Fingerprinter is most useful when deployed in an already installed plant when detailed documentation of system layout and components is not available, or shall be checked. Worldwide on-site usage - and therefore the possibility to export it to foreign countries - is essential for a wide applicability of the tool.

FF may be regarded as system for detection of stealthy intrusion, but due to the exception note it is not subject to the Wassenaar regulation for export restriction:
5.A.2.a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
Note 5.A.2.a.8. applies only to physical layer security. [5]

Flow Fingerprinter may contain technology and software developed within the US or by US citizens. If this parts exceed 10% of the total product, it is subject to US export regulation.

FF must not analyse data from networks whose owners did not allow this analysis, e.g. network of an TSO or DSO which is connected to the power plant network. Due to its method of operation, FF cannot analyse components which are e.g. behind a gateway which performs NAT or behind an application layer firewall which performs protocol conversion. To protect the plant's safety-critical control network, separation of this network with at least such measures can be assumed, therefore such an (unintended) illegal analysis is not possible.

The German Anti-Hacking forbids the creation, provision and distribution of tools which are destined for hacking. However, "friendly hacking" (penetration testing) with explicite consent ot the system owner is allowed. Because of its possible usefulness for attackers (see dual use section), FF may be within a "grey zone".

Intellectual Property Rights

Authorized usage of Flow Fingerprinter within a plant discovers only components and their versions. This information should be available for the plant operator anyway. Therefore, no IPR violation is to be expected.

Flow Fingerprinter does no reverse engineering.

Further Legal or Ethical Aspects

Usage of Open Source Software components requires analysis of the OSS licences to avoid e.g. unwanted loss of copyright.

4.5.2 Technical Aspects

Safety

Due to its passive nature, Flow Fingerprinter does not affect the plant network, and can therefore be used during all operation phases without restrictions (although it seems not useful for component design and development).

System Requirements

Flow Fingerprinter requires access to the original packets send from the component to be investigated. The packets may be encrypted, but must not be passed through gateway which changes IP header data.

Performance

Flow Fingerprinter shows - at the moment - a performance decrease for systems with more than 15 networked components. Therefore, it is suitable only for rather small networks. However, this is expected to change when the tool is further improved during the project.

4.5.3 Recommendation Summary

To further enhance to applicability of Flow Fingerprinter, we recommend to consider the following measures:

- Do not make the tool available for everybody, especially not in Germany. License it only to people who have a verifiable interest in legitimate use (e.g. penetration testers, researchers).
- Put a warning into the user manual that network owner's permission is required.
- Provide detailed documentation and warnings about effects of potential misidentifications.

- Put a standard software disclaimer in the manual and the source code.
- Keep the percentage of software with U.S. origin low, well below the de minimis limit of 10%, to stay independent of U.S. export regulation. Provide the possibility of downloading further software as plug-in if necessary.
- Get approval for distribution (export) by company legal department.
- Improve performance to allow scanning of larger networks.

4.6 Tool Distributed Network Monitoring

Distributed Network Monitoring (DNM) may be used to analyze network data which were already recorded, and to analyze network traffic live within an operating plant.

4.6.1 Ethical and Legal Aspects

Privacy

Privacy related data like email adresses of administrators and service technicians may be recorded and stored within the Distributed Network Monitoring (DNM) knowledge database.

Furthermore, timestamps of logins, work actions, and logouts can be stored, and can later potentially be misused for tracking of employee's behaviour. Therefore, privacy of such data has to be ensured when the data are recorded; analysis of the data with DNM is harmless.

Dual Use

DNM may be used in the network of an DCS by the legitimate system owner and authorized persons for discovery and documentation of system components, their communication behaviour and the network layout. DNM may also be used by an attacker for network reconnaissance by analyzing recorded network data, or by deploying an own, illegal DNM in a foreign network.

Instead of deploying own DNM components, an attacker may also intercept communication between existing DNM components, and may illegally retrieve knowledge of the network layout. Encrypting the traffic between DNM components is therefore strongly recommended to prevent illegal access to the gathered data and the derived results.

However, the attacker need to get access to the recorded data or the network to successfully use DNM; in this case, he can analyze the network and its components anyway.

Warranty

We see no warranty related issues.

Defects Liability

We see only very minor defects liability when recorded network data are analyzed: Wrong results (like misidentifications of components and faulty network layout descriptions) may give the plant operator a wrong view of the plant's network, and may cause him to perform harmful actions which the DNM manufacturer may be blamed for. However, the plant operator has the choice to verify the DNM results manually before taking critical actions.

But installing additional software like DNM on plant components may invalidate the liability of the component manufacturer; installation after the solution phase of the plant may also invalidate the liability of the plant solution provider.

Analyzing recorded data or passively listening in each network segment will not affect the plant's operation. However, the communication between components in different segments causes additional network traffic, and this may affect the plant's operation and restrict liability of the solution provider (integrator).

Trade and Usage Restrictions

DNM is most useful when deployed in an already installed plant when detailed documentation of system layout and components is not available, or shall be checked. Worldwide on-site usage - and therefore the possibility to export it to foreign countries - is essential for a wide applicability of the tool.

DNM may be regarded as system for detection of stealthy intrusion, but due to the exception note it is not subject to the Wassenaar regulation for export restriction:
5.A.2.a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;
Note 5.A.2.a.8. applies only to physical layer security. [5]

DNM seems to contain a substantial share of technology and software developed within the US or by US citizens, therefore it is likely to be subject to US export regulation.

DNM must not analyse data from networks whose owners did not allow this analysis, e.g. network of a TSO or DSO which is connected to the power plant network. Because a

DNM component has to be installed within a network segment for scanning this segment, unintended scanning of extern networks or network segments is not possible.

The German Anti-Hacking forbids the creation, provision and distribution of tools which are destined for hacking. However, "friendly hacking" (penetration testing) with explicite consent of the system owner is allowed. Because of its possible usefulness for attackers (see dual use section), DNM may be within a "grey zone".

Intellectual Property Rights

Usage of DNM shows the layout of a network. This information should be available for the plant operator anyway. Therefore, no IPR violation is to be expected.

DNM does no reverse engineering.

Further Legal or Ethical Aspects

None.

4.6.2 Technical Aspects

Safety

DNM processes already recorded data, or gathers network traffic metadata passively; this does not affect the plant network.

However, installed DNM devices in separate network segments have to communicate with each other for synchronization. This causes additional network traffic, so the DNM is not totally passive. The DNM therefore can generally be deployed in all phases of DCS operation, but is has to be taken special care that during the start-up, operation, and shut-down phase of an operating plant there is no disturbance of safety-relevant functions: The additional traffic created by the DNM has to be strongly limited, and has to be fitted within the traffic control mechanisms of the DCS, especially in the real-time critical layers.

System Requirements

DNM has to be installed in every network segment of the DCS which shall be scanned. Traffic for synchronization of different DNM components has to bypass separating firewalls which may require an adaptation of existing firewall rules.

Performance

The additional traffic created by the DNM has to be limited (see safety section).

4.6.3 Recommendation Summary

To further enhance to applicability of DNM, we recommend to consider the following measures:

- Put a warning into the user manual that network owner's permission is required.
- Provide detailed documentation and warnings about effects of potential misidentifications.
- Put a standard software disclaimer in the manual and the source code.
- Keep the percentage of software with U.S. origin low, well below the de minimis limit of 10%, to stay independent of U.S. export regulation. Provide the possibility of downloading further software as plug-in if necessary.
- Get approval for distribution (export) by company legal department.

4.7 Tool FERRET

4.7.1 Ethical and Legal Aspects

Privacy

FERRET collects forensic timestamps that can in principle be used to recreate activity logs of users (operators). However, these logs are limited and incomplete due to the fact that forensic timestamps are overwritten by the operating system. The tool also collects web access logs from which web browsing activities can be reconstructed. Though, the collection of this type of log files is configurable. Operators in plants or control systems are usually not allowed to use web access for personal use, but tracking of employee activity is generally possible with such logging data.

As it is possible to configure FERRET in a way that privacy-related data are not gathered, we highly recommend to use it in such a privacy-preserving manner by default. The corresponding configuration shall be documented and highlighted in the technical documentation and user guidelines of FERRET.

The user of FERRET shall be informed that privacy-related data may be included in gathered data, and that he has to get permission to view and analyze these data. He

must not use these data for other purposes except for the forensic analysis. Besides, he should obtain counseling from the privacy protection officer in charge before using it.

Dual Use

FERRET is a tool for data gathering and forensic analysis. It requires (physical or remote) access to the component to be analyzed. Metadata acquired by FERRET (like configuration / Windows registry, list of running processes, logfiles, etc.) are only a very minor help for hackers. Therefore, we do not regard FERRET as dual use tool for hackers.

Warranty

Installing additional software within a plant or system control network may invalidate the warranty of the solution provider (integrator), and also the system certification of regulatory authorities.

Defects Liability

FERRET requires an installation of a local agent. This must not interfere with safety critical functions running on the same device.

Trade and Usage Restrictions

FERRET uses SSH for remote access which may be subject to the Wassenaar export control list but this can be removed.

Intellectual Property Rights

Copying executables and configuration data may violate IPR of manufacturer and integrator. These data must not be used for an unauthorized reproduction of the system.

Further Legal or Ethical Aspects

Usage of Open Source Software components requires analysis of the OSS licenses to avoid e.g. unwanted loss of copyright.

4.7.2 Technical Aspects

Safety

FERRET is especially designed to gather forensic data from components (Windows computers) in real operating systems. It places a software agent on the component which runs with the lowest priority. This agent creates temporary files on the system but does not change the system configuration.

System Requirements

At the moment, FERRET is based on Windows operating system only. It requires administrative privileges for running agent executable (size about 10MB).

This agent executable can be run from the local file system, a mounted share or a USB drive. The agent creates a results file of about 60MB size at the location where it is executed, and the operator needs to be able to collect this results file from there. Alternatively, given a working network connection, the agent is able to automatically send the results to a central system.

Performance

No significant performance change is expected.

4.7.3 Recommendation Summary

To further enhance to applicability of FERRET, we recommend to consider the following measures:

- Include a privacy note in the technical documentation and user guidelines of FERRET that personal data may be included in the collected data. Permission has to be obtained before processing these data, and the data must be used for forensic analysis only.
- Describe in the technical documentation and user guidelines of FERRET how to minimize or avoid collection of privacy-related data which may be on the target device.
- Configure FERRET in a privacy-preserving manner by deactivating the retrieval of potentially privacy-related logging data in the default configuration.
- Obtain counseling from the privacy protection officer in charge before using FERRET.

- Put a warning into the user manual that permission from the plant or system operator as well as from the component manufacturer may be required before data collection can be started.
- Put a standard software disclaimer in the manual and the source code.
- Support Linux based components, too.
- Clarify share of US software, e.g. of used Open Source Software libraries
- Get approval for distribution (export) by company legal department.

5 Conclusions

The analysis showed that all tools currently developed in the CRISALIS workpackages can be used to impede or detect targeted attacks in critical infrastructures. A summary of the applicability of each tool in different life cycle phases is shown in table 5.

This includes not only the use cases "distributed control system of a power plant" (DCS) and "advanced metering infrastructure" (AMI) where CRISALIS focuses on, but also other automation szenarios such as power grids, chemical industry, pipelines, food production, and factory automation. However, the developers are highly encouraged to consider the recommendations of chapter 4.

Phase	Tool						
	Avatar	Access Miner	Smart Fuzzers	FC-Scan	FF	DNM	FER-RET
component design and development	++	++	++	o	o	o	o
component test	++	++	++	o	o	o	o
integration of components into a solution or system	o	++	o	o	++	++	o
test of integrated solution	o	++	o	o	++	++	*
comissioning of plant, field test of smart meters	–	++	–	++	++	++	*
start-up of active plant or system	–	++	–	++	++	++	++
operation of active plant or system	–	++	–	++	++	++	++
shut-down of active plant or system	–	++	–	++	++	++	++
maintenance of plant or system	–	++	–	++	++	++	++
offline analysis of a component in a test lab	++	++	++	o	o	o	o
offline analysis of recorded data from the plant	o	o	o	o	++	++	o
offline analysis of recorded data from plant components	o	o	o	o	o	o	++

Table 5.2: Applicability of CRISALIS tools in different life cycle phases:
++ high applicability;
* "readiness" (preparation) phase, required for applicability in later phases;
o not really useful or not applicable;
– must not be used due to safety reasons!

6 Annex

6.1 Questionnaire A for Tool Developers

Name of tool and tool developer	Avatar / Eurecom
Short description	Avatar is an event-based arbitration framework that orchestrates the communication between an emulator and a target physical device. Avatar's goal is to enable complex dynamic analysis of embedded firmware in order to assist in a wide range of security-related activities. The modular architecture let Avatar perform dynamic analysis of firmware behavior, such as recording and sandboxing memory accesses, performing live migration of subroutines, symbolically executing specific portion of code as well as detecting vulnerabilities.
Application area and scenario	In the context of critical infrastructures, Avatar has two main use cases: - To perform reverse engineering and dynamic analysis of modified (potentially malicious) firmwares or firmware updates. - To perform dynamic analysis and symbolic execution of embedded device firmwares with the goal of discover and mitigate possible vulnerabilities
Usage constraints	- The tool requires access to the embedded device firmware - The tool requires read/write access to the device memory (for instance through a JTAG or serial interface) - The tool requires opening of equipment chassis for installation of the backend adapter. - At this moment, the tool only supports ARM or x86 architectures
Privacy relevant data	Avatar is a dynamic analysis tool. Using Avatar, the analyst has access to everything that may be stored in the embedded device.

Export controlled functions	No crypto functions are used in Avatar
Tool development related to the US	All the development of the tool was done in France
Comments	

Name of tool and tool developer	Open source Smart Fuzzers / Security Matters
Short description	The toolset allows testing the robustness of ICS protocol implementations for a number of popular ICS and AMI protocols.
Application area and scenario	ICS/AMI equipment vendors can use the toolset during the development and quality assurance product phases, to test that the protocol implementation is robust against malformed and malicious data sent to the devices. Utility companies (e.g. energy production and distribution companies) can use the toolset to test the robustness of the ICS/AMI devices deployed in their networks. Tests can be run to assess the security of new or existing components.

Usage constraints	The toolset supports the following popular ICS/AMI protocols: - Modbus/TCP (ICS) - OPC-DA (ICS) - "PP" (ICS proprietary protocol from a major vendor) - M-BUS (AMI) The toolset implementation focuses only on testing the "server" implementation of the protocols, i.e. the device that accepts incoming TCP connections. The toolset should never be used in production environments, as this could seriously compromise the availability and security of the ICS/AMI environment. In one of our tests, the toolset caused actual physical damage to the tested equipment (i.e., a device component had to be replaced). This should be taken into account when planning the tests. Users of the toolset require a basic knowledge of the protocols being tested, since the tool needs to be configured on what protocol messages to test, and to be able to properly interpret the results of the different test cases. For example, prioritization of the test choice is important to minimize the testing time. Also, the toolset might have false positives (i.e. test cases wrongly considered failed). Some network experience is needed to understand if the failure was due to e.g. a network overload problem, or a real vulnerability found.
Privacy relevant data	The toolset does not analyze or store any privacy-relevant data.
Export controlled functions	We are not aware of any such restriction.
Tool development related to the US	The toolset requires installing the Peach fuzzing framework, which is developed and distributed free of charge by DejaVu Security, an US-based company.
Comments	The tool can be used to find vulnerabilities in existing ICS/AMI equipment. For this reason, the access to the tool has been restricted by the EU.

What test results were expected?	- Run full test for at least one device per protocol. - Identify at least one vulnerability in each of the tested devices.
What did work well? What went wrong?	- For all devices tested at least one vulnerability was found. - Most vulnerabilities lead to DoS. - One of the identified vulnerabilities might allow remote code execution (still work in progress). - Detecting faults by e.g. pinging devices does not work always (e.g. the protocol stack crashed, but the device still responds to ping). - For OPC-DA we used a driver from the OPC foundation to deliver fuzzed data to the SUT. The driver crashes during test execution because of our fuzzing. We could not get rid of the problem. This limits our ability to run the fuzzer.
What changes were required to make it work? Which changes were considered but not tested?	- To overcome the problem of detecting faults we created a new mechanism to test if the SUT failed, based on sending a valid protocol message and expecting a result after every test case. - To overcome the problem of the OPC-DA library crashing we think it will be necessary to obtain the source code of the library from the OPC foundation and fix the bug. However, we did not manage to get to the source code yet.
Which unexpected system behavior did you observe? Are there any unexpected results?	- Running a full test takes a very long time because there are many test cases and devices are slow. - Unattended tests are not possible: in case the device fails it is necessary to power cycle the device (and sometimes reconfigure it) before continuing the test.

Which effect or which system behaviour is still not understood? What has to be investigated further?	N/A
Comments	N/A

Name of tool and tool developer	FCScan / Uni Twente
Short description	FCScan is a passive monitoring tool that aims at detecting malicious electronic documents such as PDFs, Microsoft Office documents, engineering project files etc. FCScan first builds models of legitimate behavior by analyzing a number of benign samples, and then can be put into monitoring mode and flagging those documents that do not exhibit the same behavior.
Application area and scenario	FCScan can be used to monitor HMI hosts and engineering workstations, which might require the exchange of electronic documents.
Usage constraints	FCScan needs to be deployed on the host that one wishes to monitor. Application that must be monitored have to be instrumented in order to interact with FCScan.
Privacy relevant data	While FCScan might analyze sensitive information, such as username/-password pairs, it will store only abstracted information regarding the input data and therefore it's not possible to expose any sensitive information.
Export controlled functions	FCScan does not use any functions which are subject to restrictions of import/export and distribution.

Tool development related to the US	FCScan at the moment uses only the Boost library which is freely available on the Internet with unrestricted download.
Comments	

Name of tool and tool developer	Flow Fingerprinter (FF) / Uni Twente
Short description	FF is a passive fingerprinting tool that aims at recognizing ICS devices by looking at the generated traffic. The tool focuses on connections and communication patterns and creates a representation of the infrastructure under observation. FF relies on the hypothesis that "similar" ICS systems and components generate similar representations. Therefore it uses information about known devices, stored in a dataset, to recognize new ones.
Application area and scenario	FF is developed for ICS infrastructures (e.g. SCADA, DCS, etc.). The tool can be safely used in running environments for pentesting activities and security checks.
Usage constraints	FF needs to be deployed and executed on a machine with direct access (in promiscuous mode) to the ICS network. Alternatively, the tool can work on any machine that stores a Pcap dump of the ICS network traffic. No installation is needed. The hosting machine must run libpcap/winpcap libraries. No guarantee related handling are involved with the usage of FF.
Privacy relevant data	FF analyzes any data or activities within the ICS network. Depending on the ICS network infrastructure and layout, the usage of the tool can arise privacy concerns related to the supervision of company employees (e.g. login & logout times, activity recordings, etc.).
Export controlled functions	FF does not use any functions which are subject to restrictions of import/export and distribution.

Tool development related to the US	FF uses the aforementioned libpcap/winpcap and has been developed exploiting the following further libraries: jNetPcap, JUNG (Java Universal Network/Graph Framework) and JDOM. All the previous libraries are available on the Internet for free.
Comments	FF works through five different phases: 1. Gathering of information: extraction of valuable data from the traffic 2. Models construction: modeling of the ICS network 3. SCADA systems models comparison: overall assessment on the possibility to use the available dataset of fingerprints 4. Components models comparison: actual evaluation of ICS network devices traffic 5. Computation of the result: identification of ICS network components

What test results were expected?	FF was supposed to recognize most of the devices involved in a control process within an ICS network. The results were supposed to overcome the ones obtained with standard fingerprinting tools.
What did work well? What went wrong?	The preliminary tests confirmed that FF can be a valid solution to ICS fingerprinting. The tool was able to correctly recognize the majority of the devices involved in the experiments. However, still several traffic flows and communication patterns were mistakenly assigned to the wrong devices. This was due to strong similarities in the behavior of different ICS components.
What changes were required to make it work? Which changes were considered but not tested?	FF went through a continuous process of refinement of the algorithms used to create ICS network models. Moreover, the development of the metrics used to calculate similarities among models is still ongoing. Further changes in the tool are planned in conjunction with the result and the evaluation of new tests.

Which unexpected system behavior did you observe? Are there any unexpected results?	FF resulted very slow when the comparison between two ICS network models involves too many devices (> 15).
Which effect or which system behaviour is still not understood? What has to be investigated further?	Several false positives should be further investigated to understand and resolve the discriminating factors.
Comments	FF strongly relies on data availability. More tests and information from real ICS deployments are needed to validate FF fingerprinting results.

Name of tool and tool developer	Distributed Network monitoring / Symantec
Short description	The purpose of the network monitoring and discovery tool is to use low cost devices for monitoring and mapping out the layout and devices of critical infrastructure networks in a way that requires little or no modification of existing infrastructure and networks. It passively gathers network traffic metadata and from this generates network layouts and descriptions of normal traffic conditions by generating maps of which devices communicate and the patterns that are observed in their communications.

Application area and scenario	We envision this tool be used to monitor the layout of the network and be able to detect changes in the physical interconnections as well as changes in communication patterns between the various devices in the network in response to changes introduced by maintenance, outages or malicious acts.
Usage constraints	The tool requires that for each separate sub network or network segment the embedded devices are connected such that these can sniff the network traffic for that network segment or these should be connected to a span port aggregating network traffic. The devices themselves should be able to contact each other so these can share the global state of the network. This entails that in segmented networks such as where process and control networks are physically separated the systems connected to both of these networks must perform some routing/bridging function to allow these devices to communicate. At the moment we expect to utilize standard http protocols for synchronizing state between devices on a non standard port.
Privacy relevant data	Everything employees do that has a measureable effect on the monitored network is aggregated in the devices in the form of network connection meta data. So for example when and at what times an operator has initiated maintenance on devices will be recorded. To be able to label network traffic as a particular type protocol learning techniques are used to create descriptions of network traffic. It is possible for privacy relevant data to end up in such a description of a protocol learned through machine learning. For example an email address that is reused consistently may end up in the model as a constant for some protocol field.
Export controlled functions	None that we are aware of.
Tool development related to the US	Partly relies on a monitoring tool created by Symantec that collects information based on broadcast information. Contains previous work on protocol learning from Symantec
Comments	

What test results were expected?	We experimented with mapping tools for discovering the network layout of a critical infrastructure network in the hopes of getting a complete picture of devices connected to this network. For the traffic analysis portion there are two goals that we hoped to achieve, one is being able to cluster together similar messages and the other is the ability to extract some relevant variables from these messages. Hopefully so at a later stage we can use these variables for detecting changes in the physical process.
What did work well? What went wrong?	Because of the length of connections, i.e. a large number of messages without a clear beginning or ending using hierarchical clustering where the order of messages was a contributing factor to clustering messages proved impractical. Switching to flow based clustering and making some assumptions about message formats improved this situation. For interaction modeling and mapping the network layout we rely on flow based analysis more then listening for passive broadcasts.
What changes were required to make it work? Which changes were considered but not tested?	
Which unexpected system behavior did you observe? Are there any unexpected results?	

Which effect or which system behaviour is still not understood? What has to be investigated further?	
Comments	

Name of tool and tool developer	FERRET / Siemens AG
Short description	A tool for collecting forensic data from computers and PLCs, for the automated analysis of the data and for review by human analysts.
Application area and scenario	The tool is used in the investigation of potential security breaches of industrial products. Example scenarios are 1) malware infection of a computer system used for the display and evaluation of CT scan images 2) remote compromise of an industrial control system installation by hackers 3) observed miss-behavior of a turbine that could be due to a security compromise

Usage constraints	The data collection is performed by a forensic agent. The agent is able to collect forensic data from Windows based computers. The industrial product in question therefore needs to be based on and running on top of Windows. The operator needs to be able to run the agent executable file (size: 10 MB) with administrative privileges on the system. The system can continue to operate while the agent is running (runtime: about 15 min). The agent executable can be run from the local file system, a mounted share or a USB drive. The agent creates a results file of about 60MB size at the location that it was executed from and the operator needs to be able to collect this results file from there. Alternatively, given a working network connection, the agent is able to automatically send the results to a central system. The agent creates temporary files on the system but does not change the system configuration. It runs with the lowest priority.
Privacy relevant data	The tool collects forensic timestamps that can in principal be used to recreate activity logs of the users. These logs however are limited and incomplete due to the fact, that forensic timestamps gets overwritten by the operating system. The tool also collect web access logs from which web browsing activities can be reconstructed. The collection of these types of log files however is configurable.
Export controlled functions	Tool uses crypto functions of SSH for data transmission
Tool development related to the US	The tool contains various open-source components (e.g. Python programming language, Django web framework) which likely where developed with contributions from US developers but apart from this does not contain any explicit contributions from the US.
Comments	

6.2 Questionnaire B for Industrial Partners

Industrial project partner	Alliander
Which safety related issues are relevant by using the tool?	The tools should not break the underlying infrastructure that supports the AMI platform (eg. the GPRS network).
What guarantee related topics are becoming apparent by using the tool?	
What laws and regulations in the country of your residence are known to you, which could restrict usage of the tool?	Usage of the tool must be restricted to systems that we own or to systems that we have explicit permission to use. All other use is considered "computervredebreuk" under Dutch law "Wetboek van Strafrecht art. 138ab" and can lead to fines or jail sentences.

What privacy related regulations of the country of your residence may restrict the usage of the tool?	Usage of any Personal Identifiable Information must be restricted to information that we have explicit permission to use within a predefined scope. All other use is considered illegal under Dutch law "Wet Bescherming Persoonsgegevens art. 6-15" and can lead to fines.
Comment	

Industrial project partner	ENEL
Which safety related issues are relevant by using the tool?	The tools should not break the infrastructure, control systems, protection systems of machineries and humans.
What guarantee related topics are becoming apparent by using the tool?	Real Time communications/applications

What laws and regulations in the country of your residence are known to you, which could restrict usage of the tool?	Italian DSO has to guarantee Quality of Service: in Resolution 122 of 2006, the AEEG (Italian Authority for Electricity and Gas) has determined the times and ways in which to recover the service to customers affected by electricity outages in case of failure. Production: CopyRight on vendors protocols and FW/SW applications
What privacy related regulations of the country of your residence may restrict the usage of the tool?	Legislative Decree (act having the force of law) of the Italian Republic issued June 30, 2003, no. 196 and also commonly known as the "Testo unico sulla privacy". Regulate the use of private data and informations. Industrial Copy Right on Industrial systems installed in the Power Plant Legislative Decree. february 10 2005, n. 30, commonly known as the "Codice della propriet industriale". Industrial informations of the power plant production, systems etc.
Comment	

Industrial project partner	Siemens AG
Which safety related issues are relevant by using the tool?	The tools must never affect any safety relevant operations of the facility. Determining whether a tool may affect safety functions is a deeply technical question depending both on the tool and the facility system, and a general answer may be difficult.

What guarantee related topics are becoming apparent by using the tool?	Changing component firmware or pre-installed software may invalidate component manufacturer's guarantee, and may discharge the manufacturer from liability. Opening of hardware component chassis (e.g. for sensor or interface installation) may invalidate component manufacturer's guarantee, and may discharge the manufacturer from liability. Changing existing system components or adding new hardware or software components (tools) to the system may invalidate the solution provider's guarantee, and may discharge the solution provider from liability. Furthermore, even minor changes may invalidate necessary product or system certification given by regulatory authorities, and may require starting the admission process anew.
What laws and regulations in the country of your residence are known to you, which could restrict usage of the tool?	The anti-hacking clause of the German Criminal Code (Anti-Hacker-Paragraph: 202c des deutschen Strafgesetzbuches (StGB)) prohibits development and distribution of hacker tools in case of preparation of illegal hacking (202a, 202b StGB). Although developing, getting and using such tools for benevolent hacking (penetration testing explicitly authorized by the system owner) is not intended to be illegal, some security experts see there a "legal limbo". IT Security is one topic of the Wassenaar export restriction list for dual use goods. This may restrict or prevent distribution of developed Crisalis tools outside of the EU. Further investigation of this topic is necessary.
What privacy related regulations of the country of your residence may restrict the usage of the tool?	German Federal Data Protection Act (Bundesdatenschutzgesetz BDSG) regulates gathering, processing and storing of privacy related data by federal agencies and private companies. German Federal State Data Protection Acts (Landesdatenschutzgesetze) regulates gathering, processing and storing of privacy related data by federal state agencies, and companies owned by the federal states. There are further Laws and Regulations for several use cases, e.g. the Energy Industry Act (Energiewirtschaftsgesetz EnWG) or the Berlin State Hospital Act (Berliner Krankenhausgesetz), which either just reference the Federal (or a State) Data Protection Act, or specify the regulation in more detail for this use case.

Comment	Device manufacturers and solution providers require long-term support (hardware and software maintenance) for all used components. Components without such a support may not be usable for professional operation.

Bibliography

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:HTML. [last downloaded March 2014].

[2] Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens), revised bill as approved by the Lower House on 23 November 1999. http://www.dutchdpa.nl/Pages/en_wetten_wbp.aspx. [last downloaded March 2014].

[3] German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), as of June 2010. http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile. [last downloaded March 2014].

[4] Italian Personal Data Protection Code (Codice in materia di protezione dei dati personali), Legislative Decree no. 196 of 30 June 2003. http://www.privacy.it/privacycode-en.html. [last downloaded March 2014].

[5] Dual-Use List - Category 5 - Part 2 - "Information Security". http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/08%20-%20WA-LIST%20%2813%29%201%20-%20Cat%205P2.docl, December 2013. [last downloaded March 2014].

[6] Seventh Framework Programme (FP7) - Ethics check list. http://cordis.europa.eu/fp7/ethics_en.html, July 2013. [last downloaded March 2014].

[7] M. Almgren, D. Balzarotti, J. Stijohann, and E. Zambon. Deliverable D5.3: Report on automated vulnerability discovery techniques. http://www.crisalis-project.eu, May 2014.

[8] D. Balzarotti and D. Bolzoni. Deliverable D7.2: Preliminary report on host-based compromise detections. http://www.crisalis-project.eu, May 2014.

[9] M. Caselli, F. Kargl, and T. Limmer. Deliverable D5.1B: Security Testing Methodology. http://www.crisalis-project.eu, May 2014.

[10] M. Caselli, F. Kargl, and V. Tudor. Deliverable D4.4: Device Fingerprinting. http://www.crisalis-project.eu, May 2014.

[11] C. Leita. Deliverable D6.2: Protocol-agnostic approaches. http://www.crisalis-project.eu, May 2014.

[12] M. Munzert. Deliverable D2.2: Final requirement definition. http://www.crisalis-project.eu, May 2013.

[13] tba. Deliverable D7.3: Report on forensic analysis for industrial systems. http://www.crisalis-project.eu, November 2014.

Nomenclature

AEEG Italian Authority for Electricity and Gas

AMI Advanced Metering Infrastructure

ARP Address Resolution Protocol

Avatar Crisalis tool for firmware analysis of embedded devices

BDSG Bundesdatenschutzgesetz (German Federal Data Protection Act)

CDP Cisco Discovery Protocol

CR3 Control register number 3

DCS Distributed Control System

DHCP Dynamic Host Configuration Protocol

DNM Distributed Network monitoring (Crisalis tool)

DoS Denial of Service

DSO Distribution System Operator

EnWG Energiewirtschaftsgesetz (German Energy Industry Act)

FCScan Crisalis tool for document scanning

FERRET Crisalis tool for forensic data collection

FF Flow Fingerprinter - Crisalis tool for passive fingerprinting

GPRS General Packet Radio Service

HMI Human Machine Interface

http Hypertext Transfer Protocol

ICS Industrial Control Systems

IPR Intellectual Property Rights

JDOM Java library for handling of xml data

JTAG Joint Test Action Group

JTAG-port common name for IEEE 1149.1 standard test access port

JUNG Java Universal Network/Graph Framework

LLDP Link Layer Discovery Protocol

LLMNR Link-Local Multicast Name Resolution

M-BUS Meter-Bus

NAT Network Address Translation

NBNS NetBIOS Name Discovery

OLE Object Linking and Embedding

OPC-DA OLE for Process Control - Data Access

OSS Open Source Software

PLC Programmable Logic Controller

PP Proprietary Protocol

SCADA Supervisory Control And Data Acquisition

SSDP Simple Service Discovery Protocol

SSH Secure Shell

StGB Strafgesetzbuch (German Criminal Code)

STP Spanning Tree Protocol

SUT System under test

TCP Transport Control Protocol

TSO Transport System Operator